


[Web](#) [Images](#) [Groups](#) [News](#) [Froogle](#) [Local](#)<sup>New!</sup> [more »](#)

multiple packet "message authentication code"

Search

[Advanced Search](#)  
[Preferences](#)
**Web** Results 1 - 10 of about 817 for multiple packet "message authentication code" datrange:2449718-2452110. (0.32 sec)

### μTESLA Detailed Description

... μ TESLA has **multiple** phases: Sender setup, sending authenticated ... K t , to compute the **message authentication code** (MAC) of ... to ensure that the **packet** could not ...

www.ece.cmu.edu/~adrian/projects/mc2001/node18.html - 11k - [Cached](#) - [Similar pages](#)

### Introduction

... mechanism (ie appending a **message authentication code** to each ... Indeed, signing each data **packet** provides good ... a digital signature over **multiple** data packets, a ...

www.ece.cmu.edu/~adrian/projects/tesla-ndss/node1.html - 11k - [Cached](#) - [Similar pages](#)

[ [More results from www.ece.cmu.edu](#) ]

### [PPT] William Stallings Data and Computer Communications

File Format: Microsoft Powerpoint 97 - [View as HTML](#)

... Otherwise switching nodes could not read header or route **packet**. ... Useful for: Messages broadcast to **multiple** destinations. ... **Message Authentication Code**. ...

image.soongsil.ac.kr/lecture/network/Chapter\_18.ppt - [Similar pages](#)

### [PDF] Network Security Overview

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... La Tierra - Sends the same **packet** used in ... Kerberos: single sign-on to **multiple** servers

Alt ... is called a "message digest" or a **Message Authentication Code** (MAC ...

www.ecse.rpi.edu/Homework/shivkuma/teaching/sp2001/ip2001-Lecture15-6pp.pdf - [Similar pages](#)

### [PPT] Network Security

File Format: Microsoft Powerpoint 97 - [View as HTML](#)

... La Tierra - Sends the same **packet** used in a ... Kerberos: single sign-on to **multiple** servers. ... is called a "message digest" or a **Message Authentication Code** (MAC ...

www.ecse.rpi.edu/Homework/shivkuma/teaching/sp2001/ip2001-Lecture15.ppt - [Similar pages](#)

### [PDF] Header Hopping and Packet Mixers

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... a sequence number and a keyed **message authentication code** (MAC) that ... packets, and one for Alice's **packet** scheduling ... re-scheduling brackets" on multi-hop sub ...

user.it.uu.se/~tschudin/pub/cft-2000-hh.pdf - [Similar pages](#)

### Linux FreeS/WAN Glossary

... **Message Authentication Code** HMAC-SHA-96 see Hashed **Message Authentication Code** Hybrid cryptosystem A ... When a **packet** must pass over **multiple** networks, each ...

www.freeswan.org/freeswan\_trees/freeswan-1.5/doc/glossary.html - 91k - [Cached](#) - [Similar pages](#)

### [PDF] XOR MACs: New Methods for Message Authentication Using Finite ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... that virtually every transmit- ted message or **packet** will use ... M a short string, called its **message authentication code**" MAC or ... M j of M is a **multiple** of 32 ...

www-cse.ucsd.edu/~mihir/papers/xormacs.pdf - [Similar pages](#)

### List of Acronyms ----- If you think, we are missing ...

... CD - Carrier Sense **Multiple** Access - Collision ... Control MAC - **Message Authentication Code** MAN - Metropolitan ... Interconnection PAD - **Packet** Assembler Disassembler ...

ftp.cerias.purdue.edu/aux/acronyms - 11k - [Cached](#) - [Similar pages](#)

### [PDF] IRTF SMuG WG August 2000 Meeting Summary Agenda 1. Agenda bashing ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)





... in announcement protocols and the issue of having **multiple** secure groups ... of packets that use a low-cost **message authentication code** for each **packet**. ...

[www.securemulticast.org/smug9-minutes.PDF](http://www.securemulticast.org/smug9-minutes.PDF) - [Similar pages](#)

Goooooooooooooogle ►

Result Page:    1 2 3 4 5 6 7 8 9 10    **Next**

Free! Google Desktop Search: Search your own computer. [Download now.](#)

**Find:**     **emails** -  **files** -  **chats** -  **web history**

multiple packet "message authen    **Search**

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2005 Google

RFC-ED HOME	NEWS	RFC DATABASE	RFC SEARCH	RFC ERRATA	I-D SEARCH	IETF HOME
----------------	------	-----------------	---------------	---------------	---------------	--------------

# RFC Index Search Engine



## Perform Another Search :

MAC

SEARCH

Search for : All Fields Results Per Page: 25

RFC File: ☒ ASCII+ ☐ All PDFSearch : ☒ All ☐ RFC ☐ STD ☐ BCP ☐ FYIMatch : ☐ Prefix ☒ Entire WordShow Abstract: ☒ On ☐ OffShow Keywords: ☒ On ☐ OffResult Order : ☒ Descending ☐ AscendingRFC Contents Via: ☒ FTP ☐ HTTPo Based on your search of [MAC] in the *All Fields* field 12 matches were found- Below you will find matching items *1 through 12*

Number	Title	Author or Ed.	Date	Format	More Info (Obs&Upd)	Status
STD0038 RFC0903	<b>Reverse Address Resolution Protocol</b>	R. Finlayson, T. Mann, J.C. Mogul, M. Theimer	Jun-01- 1984	ASCII		STD
<b>Abstract</b>	This RFC suggests a method for workstations to dynamically find their protocol address (e.g., their Internet Address), when they know only their hardware address (e.g., their attached physical network address). This RFC specifies a proposed protocol for the ARPA Internet community, and requests discussion and suggestions for improvements.					
<b>Keywords</b>	RARP					
STD0037 RFC0826	<b>Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware</b>	D.C. Plummer	Nov-01- 1982	ASCII		STD
<b>Abstract</b>	The purpose of this RFC is to present a method of Converting Protocol Addresses (e.g., IP addresses) to Local Network Addresses (e.g., Ethernet addresses). This is an issue of general concern in the ARPA Internet Community at this time. The method proposed here is presented for your consideration and comment. This is not the specification of an Internet Standard.					
<b>Keywords</b>	ARP					
STD0036 RFC1390	<b>Transmission of IP and ARP over FDDI Networks</b>	D. Katz	January 1993	ASCII		STD
<b>Abstract</b>	This memo defines a method of encapsulating the Internet Protocol (IP) datagrams and Address Resolution Protocol (ARP) requests and replies on Fiber Distributed Data Interface (FDDI) Networks. [STANDARDS-TRACK]					
<b>Keywords</b>	IPFDDI, IEEE, 802, MAC					
RFC3664	<b>The AES-XCBC-PRF-128 Algorithm for the Internet</b>	P. Hoffman	January 2004	ASCII		PROPOSED STANDARD



	<b>Key Exchange Protocol (IKE)</b>					
<b>Abstract</b>	Some implementations of IP Security (IPsec) may want to use a pseudo-random function derived from the Advanced Encryption Standard (AES). This document describes such an algorithm, called AES-XCBC-PRF-128.					
<b>Keywords</b>	security, ipsec, advanced encryption standard, mac, message authentication code					
RFC3610	<b>Counter with CBC-MAC (CCM)</b>	D. Whiting, R. Housley, N. Ferguson	September 2003	ASCII		INFORMATIONAL
<b>Abstract</b>	Counter with CBC-MAC (CCM) is a generic authenticated encryption block cipher mode. CCM is defined for use with 128-bit block ciphers, such as the Advanced Encryption Standard (AES).					
<b>Keywords</b>	authentication, encryption, security, ciphers					
RFC3566	<b>The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec</b>	S. Frankel, H. Herbert	September 2003	ASCII		PROPOSED STANDARD
<b>Abstract</b>	A Message Authentication Code (MAC) is a key-dependent one way hash function. One popular way to construct a MAC algorithm is to use a block cipher in conjunction with the Cipher-Block-Chaining (CBC) mode of operation. The classic CBC-MAC algorithm, while secure for messages of a pre-selected fixed length, has been shown to be insecure across messages of varying lengths such as the type found in typical IP datagrams. This memo specifies the use of AES in CBC mode with a set of extensions to overcome this limitation. This new algorithm is named AES-XCBC-MAC-96. [STANDARDS TRACK]					
<b>Keywords</b>	authentication, hash security					
RFC3422	<b>Forwarding Media Access Control (MAC) Frames over Multiple Access Protocol over Synchronous Optical Network/Synchronous Digital Hierarchy (MAPOS)</b>	O. Okamoto, M. Maruyama, T. Sajima	November 2002	ASCII		INFORMATIONAL
<b>Abstract</b>	This memo describes a method for forwarding media access control (MAC) frames over Multiple Access Protocol over Synchronous Optical Network/Synchronous Digital Hierarchy (MAPOS), thus providing a way to unify MAPOS network environment and MAC-based Local Area Network (LAN) environment. This memo provides information for the Internet community.					
<b>Keywords</b>	tunneling, ethernet frames					
RFC2892	<b>The Cisco SRP MAC Layer Protocol</b>	D. Tsiang, G. Suwala	August 2000	ASCII		INFORMATIONAL
<b>Abstract</b>	This document specifies the MAC layer protocol, "Spatial Reuse Protocol" (SRP) for use with ring based media. This is a second version of the protocol (V2). This memo provides information for the Internet community.					
<b>Keywords</b>	spatial, reuse					
RFC2889	<b>Benchmarking Methodology for LAN Switching Devices</b>	R. Mandeville, J. Perser	August 2000	ASCII		INFORMATIONAL
<b>Abstract</b>	This document is intended to provide methodology for the benchmarking of local area network (LAN) switching devices. This memo provides information for the Internet community.					
<b>Keywords</b>	local, area, network, MAC, medium, access, control					
RFC2841	<b>IP Authentication using Keyed SHA1 with Interleaved Padding (IP-MAC)</b>	P. Metzger, W. Simpson	November 2000	ASCII	Obsoletes RFC1852	HISTORIC

<b>Abstract</b>	This document describes the use of keyed SHA1 (Secure Hash Algorithm) with the IP Authentication Header. This memo defines a Historic Document for the Internet community.					
<b>Keywords</b>	IPMAC, encryption, secure, hash, algorithm					
RFC2285	<b>Benchmarking Terminology for LAN Switching Devices</b>	R. Mandeville	February 1998	ASCII		INFORMATIONAL
<b>Abstract</b>	This document is intended to provide terminology for the benchmarking of local area network (LAN) switching devices. It extends the terminology already defined for benchmarking network interconnect devices in RFCs 1242 and 1944 to switching devices. This memo provides information for the Internet community. It does not specify an Internet standard of any kind.					
<b>Keywords</b>	local, area, network, MAC, Medium, Access, Control, layer					
RFC1329	<b>Thoughts on Address Resolution for Dual MAC FDDI Networks</b>	P. Kuehn	May 1992	ASCII		INFORMATIONAL
<b>Abstract</b>	In this document an idea is submitted how IP and ARP can be used on inhomogeneous FDDI networks (FDDI networks with single MAC and dual MAC stations) by introducing a new protocol layer in the protocol suite of the dual MAC stations. This memo provides information for the Internet community. It does not specify an Internet standard.					